#4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
POMET ET AL.

Serial No. **09/727,300**

Filing Date: **November 30, 2000**

For: **ELECTRONIC SECURITY COMPONENT**

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Director, U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

Transmitted herewith is a certified copy of the priority French Application No. 9915115.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Applicants

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: DIRECTOR, U.S. PATENT AND TRADEMARK OFFICE, WASHINGTON, D.C. 20231, on this 23 day of February, 2001.

This Page Blank (uspto)

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 07 DEC. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

CERTIFIED COPY OF
PRIORITY DOCUMENT

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES DATE 30 NOV 1999
LIEU 75 INPI PARIS B
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 9915115
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 30 NOV. 1999

Vos références pour ce dossier *(facultatif)* 015346 - 99-RO-211

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT
16 Avenue du Pont Royal
94230 Cachan

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	**Cochez l'une des 4 cases suivantes**
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Composant électronique de sécurité

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR		☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale		STMICROELECTRONICS SA.
Prénoms		
Forme juridique		Société Anonyme
N° SIREN		
Code APE-NAF		
Adresse	Rue	7, avenue Galliéni
	Code postal et ville	94250 GENTILLY
Pays		FRANCE
Nationalité		Française
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 NOV 1999
LIEU 75 INPI PARIS B

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 9915115

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		015346 - 99-RO-211
6 MANDATAIRE		
Nom		
Prénom		
Cabinet ou Société		CABINET BALLOT-SCHMIT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	16, avenue du Pont Royal
	Code postal et ville	94230 CACHAN
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
BORIN Lydie
Mandataire n° 94-0506
Cabinet BALLOT-SCHMIT

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

AO

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

08 113 W /260899

Vos références pour ce dossier *(facultatif)*	015346 - 99-RO-211
N° D'ENREGISTREMENT NATIONAL	99 15 115

TITRE DE L'INVENTION (200 caractères ou espaces maximum)
Composant électronique de sécurité

LE(S) DEMANDEUR(S) :
STMICROELECTRONICS SA.
7, avenue Galliéni
94250 Gentilly

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		POMET	
Prénoms		Alain	
Adresse	Rue	domicilié au Cabinet BALLOT-SCHMIT 16, avenue du Pont Royal	
	Code postal et ville	94230	CACHAN
Société d'appartenance *(facultatif)*			
Nom		PLESSIER	
Prénoms		Bernard	
Adresse	Rue	domicilié au Cabinet BALLOT-SCHMIT 16, avenue du Pont Royal	
	Code postal et ville	94230	CACHAN
Société d'appartenance *(facultatif)*			
Nom		SOURGEN	
Prénoms		Laurent	
Adresse	Rue	domicilié au Cabinet BALLOT-SCHMIT 16, avenue du Pont Royal	
	Code postal et ville	94230	CACHAN
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)

BORIN Lydie
Mandataire n° 94-0506
Cabinet BALLOT-SCHMIT

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

AO

COMPOSANT ELECTRONIQUE DE SECURITE

La présente invention concerne un composant électronique de sécurité. Elle concerne toutes les applications dans lesquelles des informations sensibles sont traitées.

De tels composants sont notamment utilisés dans des cartes à puces, pour certaines applications de celles-ci, par exemple pour l'accès à des banques de données, pour des applications bancaires, ou encore des applications de télé péage pour la télévision, la distribution d'essence ou le passage de péages d'autoroutes.

Ces composants sont amenés à traiter des données confidentielles, qu'il faut préserver de toute tentative d'espionnage aux fins de fraude. Ces données confidentielles transitent par le bus de données du composant, entre une unité centrale de traitement (processeur) et des périphériques tels que des mémoires.

Or différents moyens peuvent être mis en oeuvre pour découvrir ces données confidentielles. Notamment, une caractéristique physique observable de l'extérieur du composant électronique est sa signature en courant, fonction des transitions sur le bus de données. En effet, le bus de donnée à une grosse capacité du fait qu'il circule dans tout le composant. Pour cette raison, l'interface de sortie comprend des commutateurs trois états dimensionnés pour passer un fort courant, permettant de charger ou décharger la capacité de ligne. S'agissant d'un bus de données 8 bits, ce sont alors 8 gros commutateurs qui sont activés pour appliquer une donnée sur ce bus, avec une consommation en courant importante à la commutation.

Un objet de l'invention est d'empêcher ou de rendre plus difficile la détermination des données qui transitent sur le bus.

Un objet de l'invention est d'utiliser le cryptage des données pour améliorer la protection des données confidentielles.

Un autre objet de l'invention, est de mettre en oeuvre un cryptage de données d'une manière peu coûteuse, que ce soit en surface silicium, en lignes de connexion entre les périphériques et l'unité centrale et en temps de traitement des données.

Un autre objet de l'invention est de mettre en oeuvre un cryptage de données adaptable à toutes les familles de composant de façon simple, sans surcoût de conception personnalisée.

Une solution à ces différents problèmes techniques a été trouvée dans l'invention dans un composant dont l'unité centrale et les périphériques ayant à traiter des données sensibles reçues ou transmises sur le bus de données comprennent chacun une cellule de cryptage/décryptage et qui applique à une donnée reçue ou à transmettre dans un cycle horloge une même clé secrète produite localement par chaque cellule, à chaque cycle horloge.

Si on retient la convention selon laquelle un cycle horloge débute sur le niveau haut, l'écriture d'une donnée sur le bus se fait sur le niveau bas et la lecture d'une donnée sur le bus se fait sur le front montant. Ainsi, dans un cycle d'horloge donné, une donnée peut être cryptée avec une clé secrète produite par la cellule d'un émetteur et transmise sur le bus pendant la période d'écriture sur le bus et cette donnée cryptée peut être lue par un destinataire et décryptée dans la cellule de ce destinataire avec la

clé secrète produite localement par cette cellule, les deux clés secrètes produites localement ayant la particularité d'être identiques. Ainsi, selon l'invention, la clé secrète est produite localement dans chaque cellule à partir d'un signal aléatoire synchrone appliqué à toutes, pour servir dans un même cycle horloge au cryptage d'une donnée fournie par un émetteur et au décryptage de cette donnée cryptée par un destinataire.

Telle que caractérisée, l'invention concerne donc un composant électronique comprenant un bus bidirectionnel par lequel transitent des données entre des périphériques et une unité centrale à la cadence d'un signal d'horloge, caractérisé en ce que l'unité centrale et au moins l'un des périphériques comprennent chacun une cellule de cryptage/décryptage des données utilisant une même clé secrète, une valeur courante de ladite clé secrète étant produite localement dans chaque cellule à chaque cycle horloge à partir d'un signal aléatoire synchrone du signal d'horloge, appliqué à chacune des cellules par une ligne de transmission unidirectionnelle.

D'autres caractéristiques et avantages de l'invention sont détaillés dans la description suivante à titre indicatif et non limitatif, et en référence aux dessins annexés dans lesquels :

- la figure 1 représente un exemple d'architecture d'un composant électronique auquel l'invention peut s'appliquer;
- la figure 2 représente une architecture simplifiée d'un composant électronique selon l'invention;

- la figure 3 est un exemple de chronogramme des signaux de données et de commande du composant électronique représenté à la figure 2 ;
- la figure 4 est un schéma bloc d'une cellule de cryptage/décryptage selon l'invention ;
- la figure 5 représente la cellule de cryptage/décryptage comprenant un circuit conditionnel selon un perfectionnement de l'invention, applicable à l'unité centrale;
- la figure 6 est un schéma détaillé des moyens de cryptage et de décryptage dans une cellule et;
- la figure 7 représente un schéma bloc d'un générateur de signal aléatoire synchrone qui peut être utilisé dans l'invention.

La figure 1 représente un exemple d'architecture d'un composant électronique de sécurité auquel l'invention peut s'appliquer. Dans cet exemple, le composant électronique est plus particulièrement destiné aux applications de type carte à puce. Ses connexions externes se limitent ainsi à deux plots d'entrée/sortie série, un plot horloge CLK pour recevoir un signal d'horloge externe, un plot pour recevoir un signal d'initialisation RST et les plots d'alimentation logique, Vcc et Gnd.

L'architecture de ce composant comprend une unité centrale CPU, et des périphériques P1, P2, P3, qui sont dans l'exemple, respectivement, une mémoire non volatile, par exemple de type EEPROM, une mémoire de travail de type RAM et une mémoire programme, de type ROM.

Un circuit d'interface INT assure l'interface entre les plots d'entrée/sortie série et le bus parallèle du composant qui se décompose en un bus d'adresse, AD-BUS

et un bus de donnée DATA-BUS auxquels sont connectés l'unité centrale et les périphériques.

Dans cette architecture, on a aussi prévu un circuit CAP de contrôle d'accès au périphérique qui reçoit les bits de poids forts A7-A5 du bus d'adresse AD-BUS. Il contient une table d'allocation de l'espace physique adressable du composant et fournit notamment les signaux de sélection P1-sel, P2-sel et P3-sel des périphériques P1, P2, P3, en fonction de l'adresse décodée. Dans cette exemple, les périphériques ne reçoivent que les bits de poids faibles A5-A0 du bus d'adresse.

En fonction des instructions que l'unité centrale reçoit de l'extérieur, elle fournit des signaux de contrôle CTL, notamment, un signal de lecture/écriture RW, appliqués aux périphériques. Enfin, le plot CLK fournit le signal d'horloge PHI appliqué à tous les circuits du composant, soit dans l'exemple à l'unité centrale, aux périphériques, au circuit d'interface et au circuit de contrôle d'accès aux périphériques.

Dans l'invention, on cherche à sécuriser ce circuit, en empêchant la détermination des données qui transitent sur le bus de donnée interne DATA-BUS, par observation de la consommation en courant du composant.

Ainsi, comme représenté sur la figure 2, dans une représentation simplifiée de l'architecture du composant de la figure 1, on place une cellule de cryptage/décryptage dans l'unité centrale et dans chacun des périphériques qui lisent ou écrivent des données sensibles sur le bus de données, dans l'exemple, dans les périphériques P1 et P2. Ces cellules sont référencées $Kcell_{CPU}$, $Kcell_{P1}$ et $Kcell_{P2}$ sur la figure 2.

Le composant électronique selon l'invention comprend alors un générateur d'un signal aléatoire KIN, synchrone du signal d'horloge, sur une ligne de transmission unidirectionnelle, pour appliquer ce signal à chacune des cellules de cryptage/décryptage prévues dans le composant.

Chacune de ces cellules est en outre connectée en entrée/sortie au bus de données DATA-BUS.

La figure 3 représente un chronogramme correspondant à une opération de lecture par l'unité centrale d'une donnée du périphérique P1 suivie d'une opération d'écriture d'une donnée par l'unité centrale dans le périphérique P1.

Ce chronogramme permet d'illustrer le principe de l'invention.

On a représenté sur ce chronogramme, deux cycles d'horloge, notés cycle 1 et cycle 2, le signal aléatoire synchrone KIN , la clé secrète KEY calculée localement dans chaque cellule, le bus d'adresse AD-BUS, le signal de sélection P1-sel du périphérique P1, le signal de commande de lecture/écriture RW, dont le niveau bas correspond a une commande d'écriture, et le niveau haut, à une commande de lecture (par convention), et le bus de donnée DATA-BUS.

Si on considère le premier cycle horloge représenté (cycle 1), il lui correspond une valeur KEY_0 de clé secrète calculée localement dans chaque cellule à partir de la nouvelle valeur entrante du signal aléatoire KIN, 0 dans l'exemple.

Le périphérique P1 est sélectionné (P1-sel au niveau haut) en lecture (RW au niveau haut) à l'adresse appliquée sur le bus d'adresse AD-BUS. La cellule $Kcell_{P1}$ du périphérique P1 fournit sur le bus la donnée lue à cette adresse, cryptée au moyen de la valeur

courante de clé secrète KEY_0 calculée localement par cette cellule $Kcell_{P1}$. Cette donnée est transmise sur le bus sur le niveau bas du cycle 1 du signal d'horloge. La donnée cryptée est mémorisée dans un registre d'entrée de l'unité centrale CPU sur le front montant du cycle 1 du signal d'horloge et décryptée par la cellule $Kcell_{CPU}$, en utilisant la valeur courante KEY_0 de la clé secrète calculée localement par cette cellule $Kcell_{CPU}$.

Si on considère le deuxième cycle horloge représenté (cycle 2), il lui correspond une valeur KEY_1 de clé secrète calculée localement dans chaque cellule à partir de la nouvelle valeur entrante du signal aléatoire KIN, 1 dans l'exemple.

Le périphérique P1 est sélectionné (P1-sel au niveau haut) en écriture (RW au niveau bas) à l'adresse appliquée sur le bus d'adresse AD-BUS. La cellule $Kcell_{CPU}$ de l'unité centrale fournit sur le bus la donnée à écrire à cette adresse, cryptée au moyen de la valeur courante de clé secrète KEY_1 calculée localement par cette cellule $Kcell_{CPU}$. Cette donnée est transmise sur le bus sur le niveau bas du cycle 2 du signal d'horloge. La donnée cryptée est mémorisée dans un registre d'entrée du périphérique P1 sur le front montant du cycle 2 du signal d'horloge et décryptée par la cellule $Kcell_{P1}$, en utilisant la valeur courante KEY_1 de la clé secrète calculée localement par cette cellule $Kcell_{P1}$.

Un schéma bloc général d'une cellule de cryptage/décryptage Kcell selon l'invention est représenté sur la figure 4. Cette cellule est telle qu'elle calcule localement la valeur courante de la clé secrète, utilisée aussi bien pour le cryptage que pour le décryptage.

La cellule Kcell comprend un registre KEYREG, qui fournit la clé secrète KEY utilisée pour le cryptage et le décryptage. C'est un registre à décalage à n étages séquencé par le signal d'horloge PHI et qui reçoit en entrée de donnée le signal aléatoire KIN synchrone du signal d'horloge PHI. Le registre KEYREG fournit en sortie la valeur courante de la clé secrète KEY, pour le cycle d'horloge courant, dont la valeur est une fonction polynomiale des n valeurs les plus récentes du signal aléatoire KIN. La clé secrète prend ainsi une nouvelle valeur aléatoire à chaque cycle horloge.

Le registre est de préférence un registre à décalage à rétroaction, c'est à dire comprenant des portes logiques combinatoires pour appliquer le bit de sortie de certains étages en entrée d'autres étages du registre. Ceci permet de façon bien connue d'obtenir des fonctions polynomiales intéressantes. De préférence, on choisira d'implémenter une fonction polynomiale irréductible, pour améliorer la résistance du cryptage.

La cellule Kcell comprend un module A de cryptage et un module B de décryptage auxquels est appliquée la clé secrète KEY fournie par le registre KEYREG de la cellule.

Dans l'exemple, la fonction mathématique mise en oeuvre dans le module de cryptage est la fonction OU exclusif qui a la particularité d'être aussi la fonction à appliquer dans le module de décryptage, et d'être d'une mise en oeuvre aisée.

Le module A de cryptage reçoit en entrées une donnée interne Dout du circuit dans lequel est placée la cellule Kcell, et la clé secrète KEY produite localement par le registre KEYREG. Il délivre en sortie une donnée cryptée appliquée sur le bus de donnée DATA-

BUS, via l'interface de sortie du circuit, symboliquement représenté sur la figure par un inverseur commandé.

Le module B de décryptage reçoit une donnée du bus de donnée, et la clé secrète KEY produite localement par le registre KEYREG. Il fournit en sortie une donnée décryptée Din.

Dans un perfectionnement représenté sur la figure 5, la cellule de cryptage/décryptage de l'unité centrale comprend en plus des éléments précédemment décrits, un circuit conditionnel, qui permet d'appliquer aux modules de cryptage et de décryptage, soit la clé secrète KEY soit une clé neutre KN, correspondant au neutre pour l'opération de cryptage considérée. Dans l'exemple de l'opération OU exclusif, ce neutre est la valeur nulle.

Ce perfectionnement permet de ne pas devoir implémenter une cellule de cryptage/décryptage dans tous les circuits connectés au bus de données dans le composant considéré, mais dans seulement ceux qui manipulent des données à protéger. On prévoit donc que le circuit PAC de contrôle d'accès des périphériques (représenté sur les figures 1 et 2) fournit un signal de validation de cryptage SCRAMBLE vers l'unité centrale CPU à chaque fois qu'il décode l'adresse d'un tel périphérique. En pratique, ce circuit de contrôle d'accès trouve cette information dans sa table d'allocation des adresses physiques.

On notera que l'information SCRAMBLE est dans l'exemple fournie par un circuit de contrôle d'accès placé en dehors de l'unité centrale, dans l'exemple d'architecture représenté sur les figures 1 et 2. Ceci n'est absolument limitatif. L'information SCRAMBLE est

de façon plus générale fournie par un circuit de décodage d'adresse du composant.

Le circuit conditionnel de la cellule $KCell_{CPU}$ selon le perfectionnement de l'invention comprend un multiplexeur MUX recevant en entrées la clé secrète KEY et la clé neutre KN et fournit en sortie la clé sélectionnée par le signal de validation de cryptage SCRAMBLE, appliquée aux modules de cyrptage et de décryptage de cette cellule $Kcell_{CPU}$.

La figure 6 représente de façon un peu plus détaillée une cellule de cryptage/décryptage selon l'invention. Si on considère un bus de données 8 bits, la clé secrète doit comprendre au moins autant de bits. Le registre KEYREG comprend ainsi 8 étages pour fournir 8 bits de clé secrète, notés K0 à K7. Chacun de ces huit bits de données est appliqué dans le module A de cryptage et dans le module B de décryptage à une porte OU exclusif correspondante, recevant en entrée le bit de donnée à crypter ou décrypter, de même ordre. Ces modules comprennent ainsi chacun huit portes ou exclusif, une par bit.

Sur cette figure, on a représenté un exemple de réalisation d'un registre KEYREG du type à décalage, à rétroaction. On note E0 à E7 les 8 étages du registre, fournissant respectivement les bits K7 à K0 de la clé secrète. Ces étages sont de manière bien connue, des bascules de type D (flip-flop).

Dans l'exemple de réalisation représenté, l'étage E0 reçoit en entrée le signal aléatoire KIN combiné dans une porte OU exclusif au bit K0 fourni par le dernier étage E7 du registre, et délivre en sortie le bit K7. L'étage E1 reçoit en entrée le bit K7 combiné dans une porte OU exclusif au bit K0, et délivre en sortie le bit K6. Les étages E2, E3 et E4 reçoivent en entrée le

bit fourni par l'étage précédent et délivrent en sortie les bits K5, K4 et K3 respectivement. L'étage E5 reçoit en entrée le bit K3 combiné dans une porte OU exclusif au bit K0, et délivre en sortie le bit K2. L'étage E6 reçoit en entrée le bit K2 combiné dans une porte OU exclusif au bit K0, et délivre en sortie le bit K1. L'étage E7 reçoit en entrée le bit K1 et délivre en sortie le bit K0.

La figure 7 représente un exemple d'un générateur KEYGEN du signal aléatoire KIN.

Dans cet exemple, le générateur comprend un générateur pseudo aléatoire pour fournir une horloge aléatoire qui est appliquée en entrée D d'une bascule BS, pour être resynchronisée par le signal d'horloge PHI. Cette bascule reçoit donc sur son entrée horloge, le signal d'horloge PHI, et fournit en sortie Q, un signal aléatoire KIN synchrone du signal d'horloge PHI.

Il est a priori très difficile de déterminer la valeur prise par le signal aléatoire par observation de la consommation du composant due aux commutations sur la ligne de transmission du signal aléatoire synchrone KIN, car la capacité de cette ligne unidirectionnelle est en pratique assez faible.

Néanmoins, dans un perfectionnement de l'invention, on prévoit que le générateur du signal aléatoire synchrone comprend un circuit CMC de masquage de la consommation due aux commutations sur cette ligne de transmission. Dans l'exemple, ce circuit CMC est connecté entre la sortie de la bascule de synchronisation BS et la ligne de transmission.

Il existe différents circuits de masquage de consommation plus ou moins performants. Un exemple de réalisation non exhaustif est représenté sur la figure 5. Il comprend deux bascules de type D, B1 et B2. La

première bascule B1 reçoit en entrée de donnée, la sortie Q de la bascule de synchronisation BS, et en entrée horloge, le signal d'horloge du bus PHI. La sortie Q est connectée par un élément d'interface (*driver*) I1 à la ligne de transmission. La sortie complémentaire /Q de la bascule B1 est appliquée à un circuit combinatoire dont la sortie S est appliquée en entrée de donnée de la deuxième bascule B2. La sortie Q de cette deuxième bascule B2 est connectée à un condensateur CKN dont la capacité correspond à la capacité parasite CK de la ligne de transmission vue par l'interface de sortie I1 du générateur KEYGEN.

Le circuit combinatoire comprend dans l'exemple une première porte OU recevant en entrées les sorties Q de la bascule de synchronisation et de la deuxième bascule B2 et une deuxième porte OU recevant en entrées la sortie de la première porte et la sortie complémentaire /Q de la première bascule B1. Avec un tel circuit combinatoire, on obtient dans les bascules B1 et B2 des transitions complémentaires, en sorte que la même consommation due à la transmission du signal KIN est observée à chaque cycle horloge.

Dans un dernier perfectionnement de l'invention, on prévoit que le signal aléatoire KIN n'est transmis sur la ligne de transmission qu'après activation par l'unité centrale d'un signal EN-ENCRYPT d'activation du cryptage. Ceci peut se faire simplement en forçant la réinitialisation des bascules. On a ainsi représenté sur la figure 7 une porte logique de type ET recevant en entrées le signal de réinitialisation RST du composant, actif à zéro, et le signal de validation EN-ENCRYPT. Ce signal est à zéro par défaut. Ainsi, après l'initialisation, tant que le signal de validation est à zéro, les bascules B1 et B2 sont forcées à zéro, et

la ligne de transmission est forcée à zéro. Dès qu'il est mis à 1 par l'unité centrale, le signal aléatoire est transmis.

On notera que les deux perfectionnements du générateur du signal aléatoire synchrone, à savoir, le masquage de la consommation et la validation du cryptage, peuvent être mise en oeuvre indépendamment l'une de l'autre. Ainsi, dans certains composants, on pourra mettre en œuvre un seul de ces perfectionnements. A cet effet, on notera que le perfectionnement concernant la validation du cryptage peut être mis en oeuvre indépendamment du circuit de masquage, par exemple au moyen d'une porte logique ET recevant en entrées le signal aléatoire synchrone KIN et le signal d'activation EN-ENCRYPT, et connecté en sortie sur la ligne de transmission.

Avec l'utilisation de cellules de cryptage/décryptage selon l'invention, on obtient ainsi une protection efficace des données sensibles. Cette protection est peu coûteuse en termes de conception, d'implémentation et de temps de traitement dans le composant. Notamment, la conception est facilitée par l'utilisation de cellules de cryptage/décryptage identiques dans tous les périphériques. La cellule de cryptage/décryptage de l'unité centrale comprend une option de validation du cryptage permettant de ne pas implanter une cellule nécessairement sur tous les périphériques. Le générateur du signal aléatoire quant à lui comprend deux options de réalisation, une option de masquage de consommation et une option d'activation de cryptage/décryptage.

REVENDICATIONS

1. Composant électronique comprenant un bus bidirectionnel (DTA-BUS) par lequel transitent des données entre des périphériques (P1, P2, P3) et une unité centrale (CPU) à la cadence d'un signal d'horloge (PHI), caractérisé en ce que l'unité centrale (CPU) et au moins l'un des périphériques (P1) comprennent chacun une cellule de cryptage/décryptage (Kcell) des données utilisant une même clé secrète (KEY), une valeur courante de ladite clé secrète étant produite localement à chaque cycle horloge dans chaque cellule à partir d'un signal aléatoire (Kin) synchrone du signal d'horloge (PHI), et appliqué à chacune des cellules par une ligne de transmission unidirectionnelle.

2. Composant électronique selon la revendication 1, caractérisé en ce que chaque cellule comprend un registre à décalage (KEYREG) recevant en entrée de donnée, ledit signal aléatoire synchrone (KIN) et en entrée horloge, le signal d'horloge (PHI) et délivrant en sortie, une valeur courante (KEY_0) de clé secrète à chaque cycle horloge.

3. Composant électronique selon la revendication 2, caractérisé que ledit registre à décalage est du type à rétroaction.

4. Composant électronique selon la revendication 3, caractérisé en ce que la fonction polynomiale correspondante du registre est irréductible.

5. Composant électronique selon l'une des revendications 1 à 4, caractérisé en ce que chaque

cellule de cryptage/décryptage (Kcell) comprend un module de cryptage (A) recevant en entrées la valeur courante (KEY_0) de la clé secrète et une donnée (Dout) à transmettre sur le bus, pour fournir en sortie une donnée cryptée, et un module de décryptage (B) recevant en entrées la valeur courante (KEY_0) de la clé secrète et une donnée reçue du bus pour délivrer en sortie une donnée décryptée (Din).

6. Composant électronique selon la revendication 5, caractérisé en ce que la cellule de cryptage/décryptage ($Kcell_{CPU}$) de l'unité centrale (CPU) comprend en outre un circuit conditionnel pour appliquer la valeur courante de la clé secrète ou une clé neutre (KN) aux dits modules de cryptage (A) et de décryptage (B) selon un signal de validation de cryptage (SCRAMBLE) fourni par un circuit de décodage d'adresse (CAP) du composant.

7. Composant électronique selon la revendication 5 ou 6, caractérisé en ce que le module de cryptage et le module de décryptage utilisent la même fonction mathématique.

8. Composant électronique selon l'une quelconque des revendications précédentes, caractérisé en ce qu'un générateur dudit signal aléatoire synchrone (KIN) comprend un circuit (CMC) de masquage de la consommation.

9. Composant électronique selon la revendication 8, caractérisé en ce que ledit générateur comprend une bascule de type D (BS) recevant en entrée de donnée un signal binaire aléatoire et sur l'entrée horloge, le signal d'horloge du bus, pour fournir en sortie le

signal aléatoire synchrone (KIN) et en ce que le circuit de masquage de consommation est connecté entre la sortie de la dite bascule et la ligne de transmission.

10. Composant électronique selon l'une quelconque des revendications précédentes, caractérisé en ce que ladite ligne de transmission du signal aléatoire synchrone (KIN) est forcée à zéro par défaut par l'unité centrale (CPU), un générateur de ce signal comprenant un circuit logique pour ne transmettre ledit signal aléatoire synchrone (KIN) sur la ligne de transmission qu'après activation d'un signal de commande (EN-ENCRYPT) par l'unité centrale.

11. Système comprenant un composant électronique selon l'une quelconque des revendications précédentes.

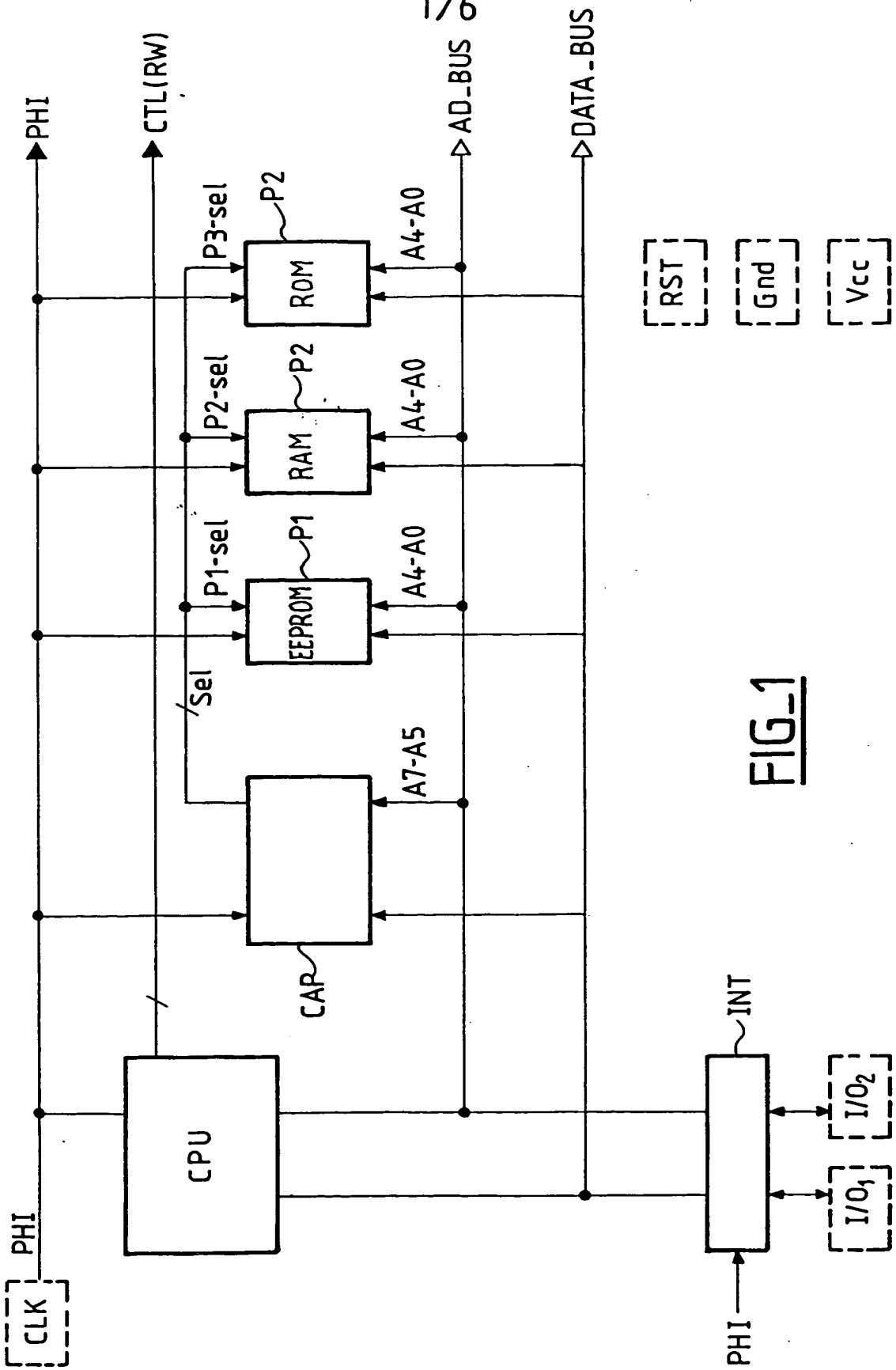

PHI
CTL(RW)
AD_BUS
DATA_BUS
P3-sel
P2
ROM
A4-A0
P2-sel
P2
RAM
A4-A0
P1-sel
P1
EEPROM
A4-A0
Sel
A7-A5
CAP
INT
CPU
PHI
CLK
PHI
RST
Gnd
Vcc
I/O2
I/O1

FIG_1

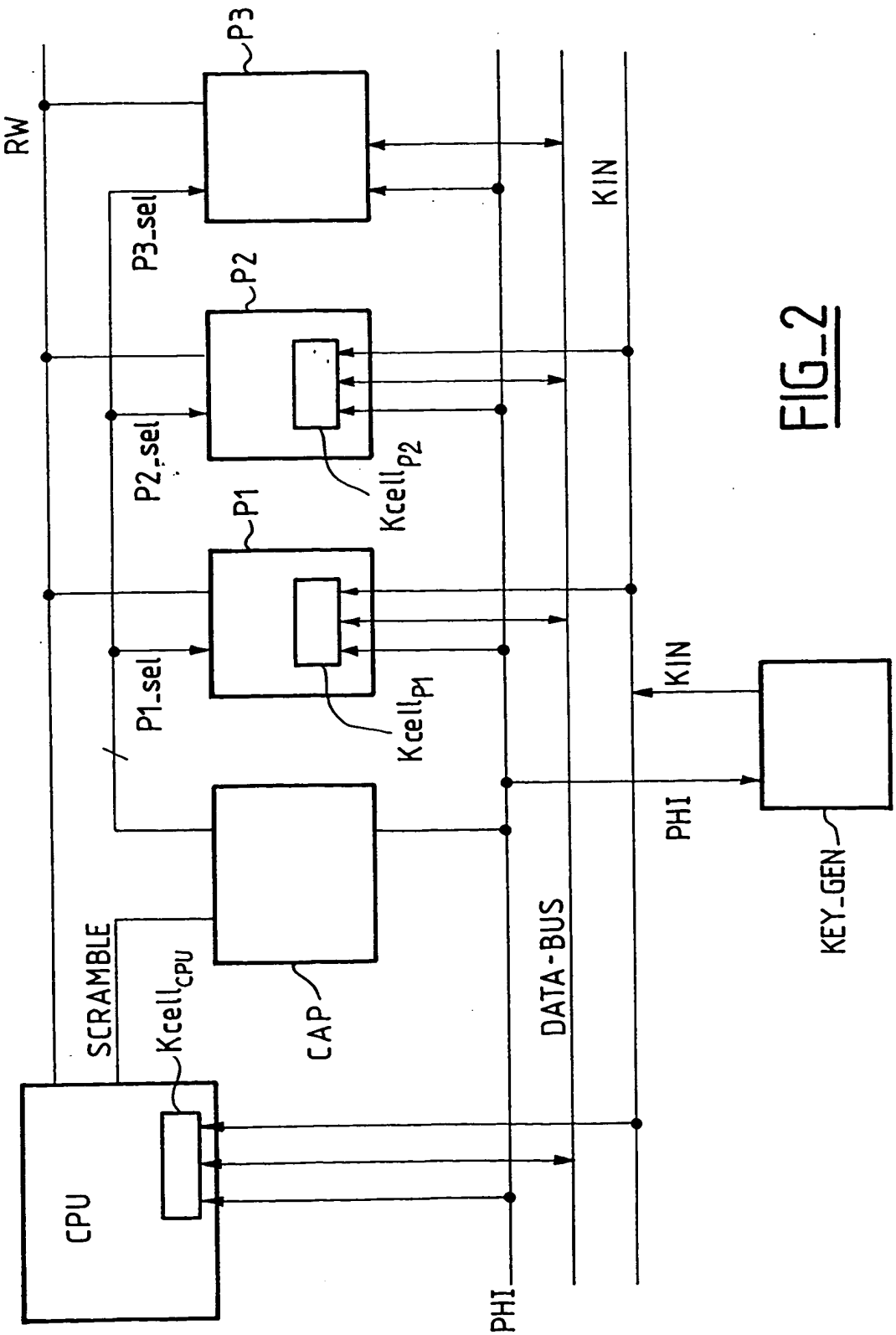

RW
P3
P3_sel
P2
P2_sel
Kcell$_{P2}$
P1
P1_sel
Kcell$_{P1}$
KIN
KIN
PHI
KEY_GEN
SCRAMBLE
Kcell$_{CPU}$
CAP
DATA-BUS
CPU
PHI

FIG_2

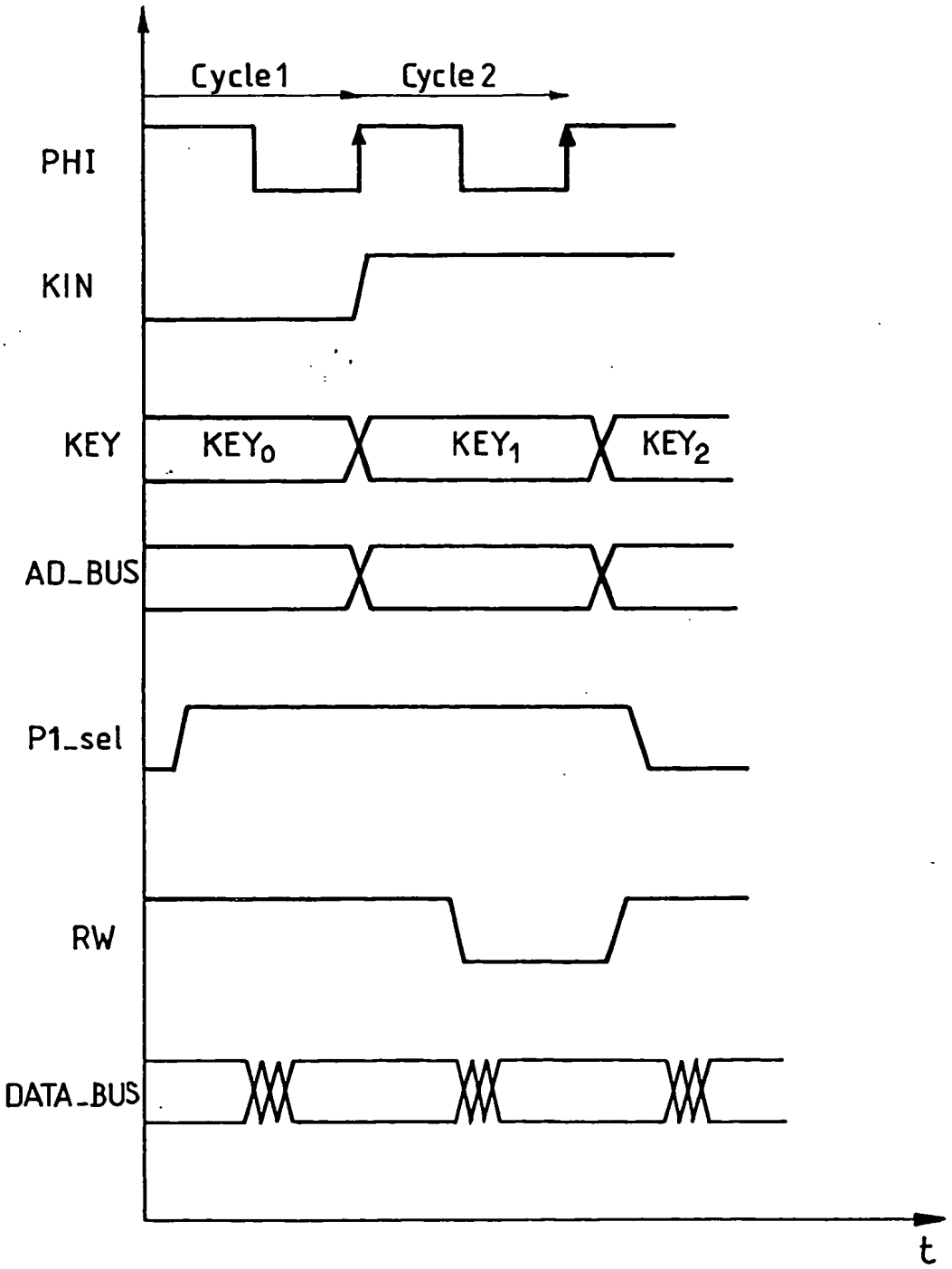

Cycle1
Cycle2
PHI
KIN
KEY
KEY0
KEY1
KEY2
AD_BUS
P1_sel
RW
DATA_BUS
t

FIG_3

FIG_4

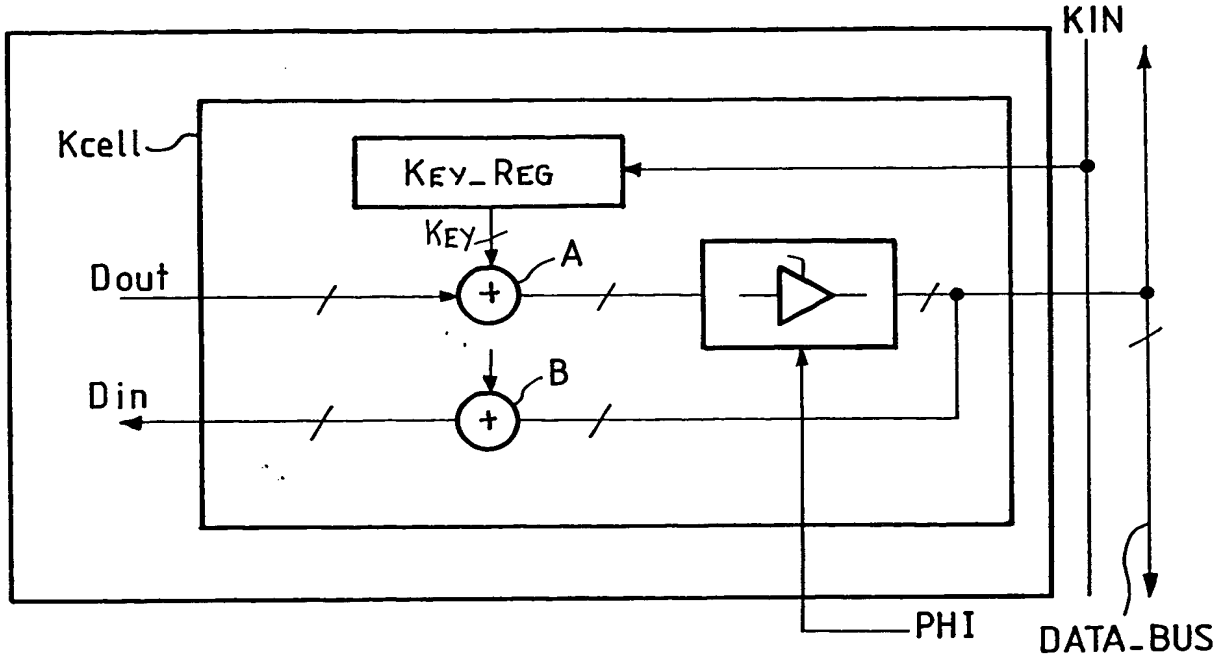

KIN
Kcell
KEY_REG
KEY
A
Dout
B
Din
PHI
DATA_BUS

FIG_5

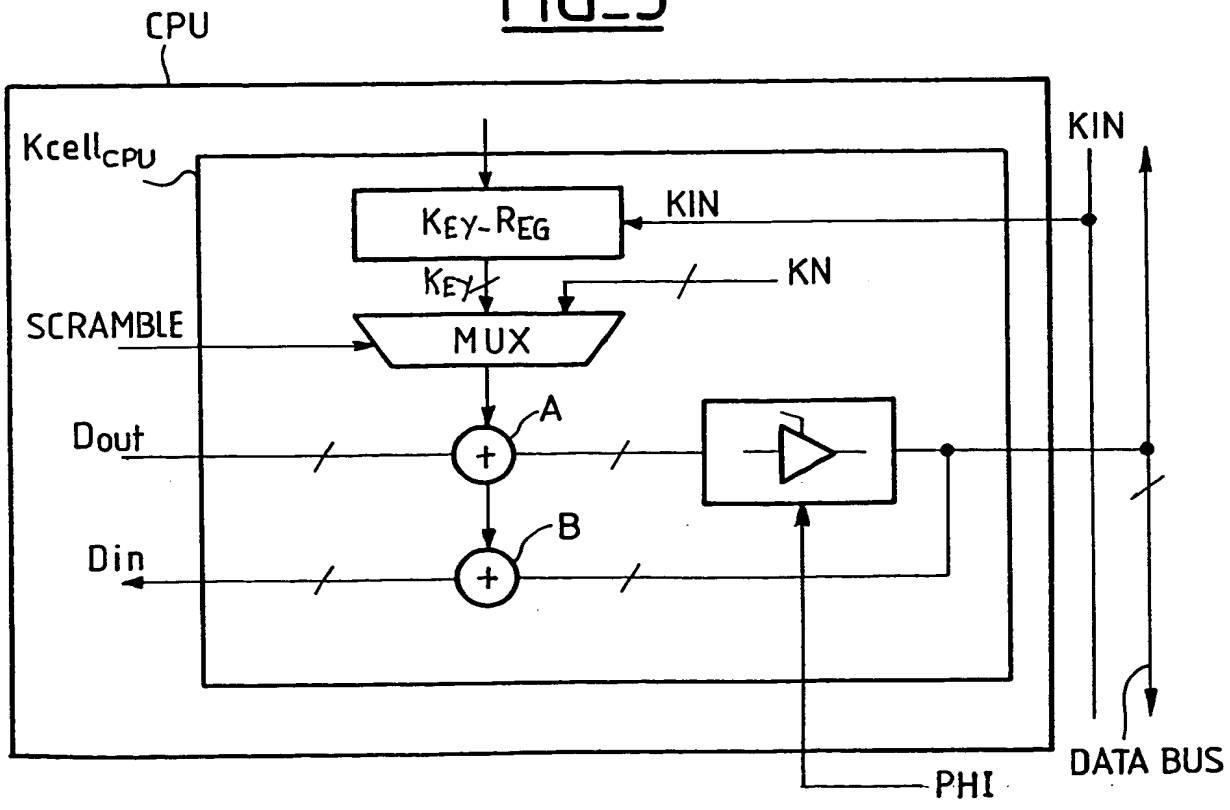

CPU
KIN
KcellCPU
KEY-REG
KIN
KEY
KN
SCRAMBLE
MUX
A
Dout
B
Din
PHI
DATA BUS

FIG_6

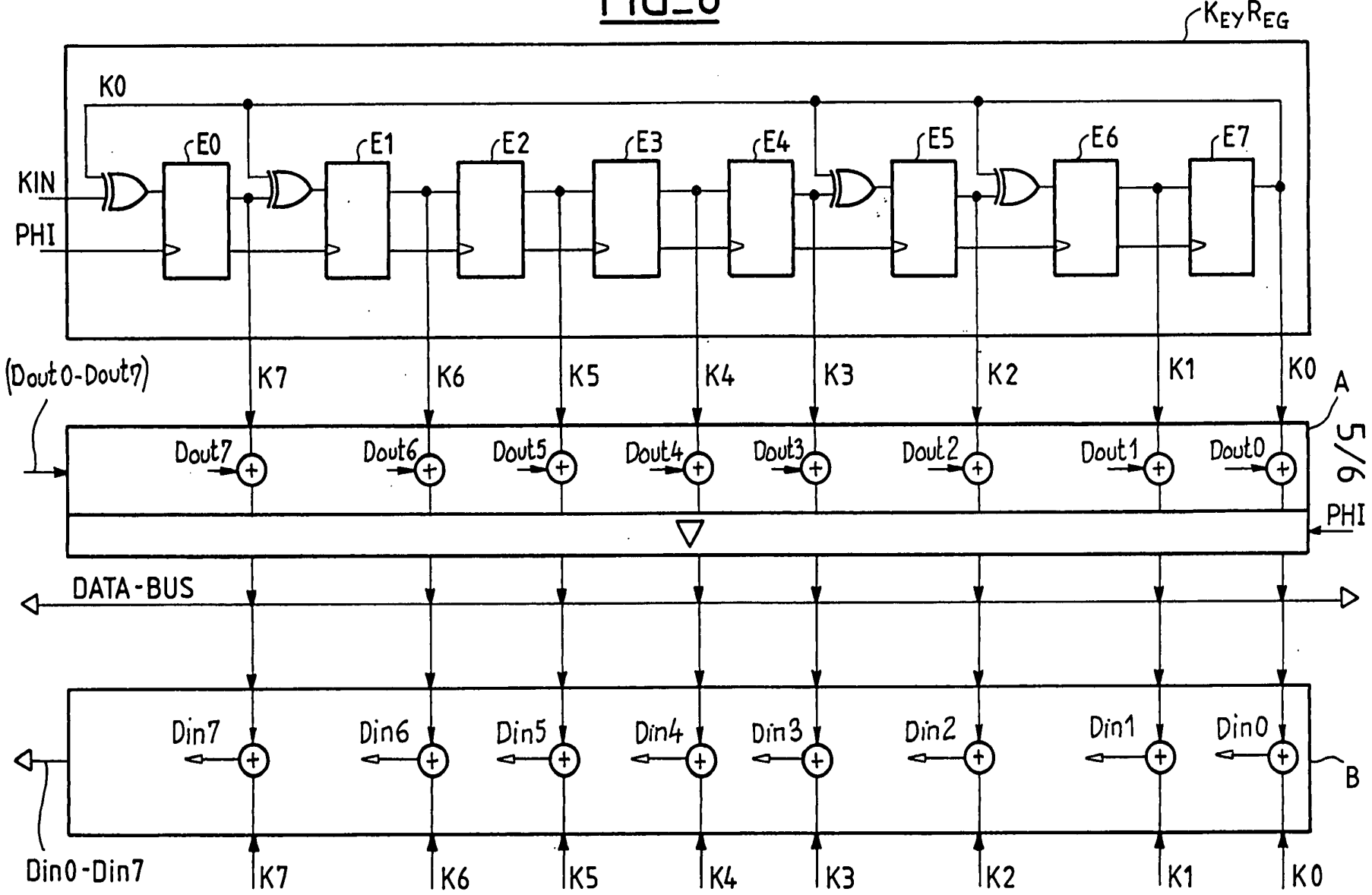
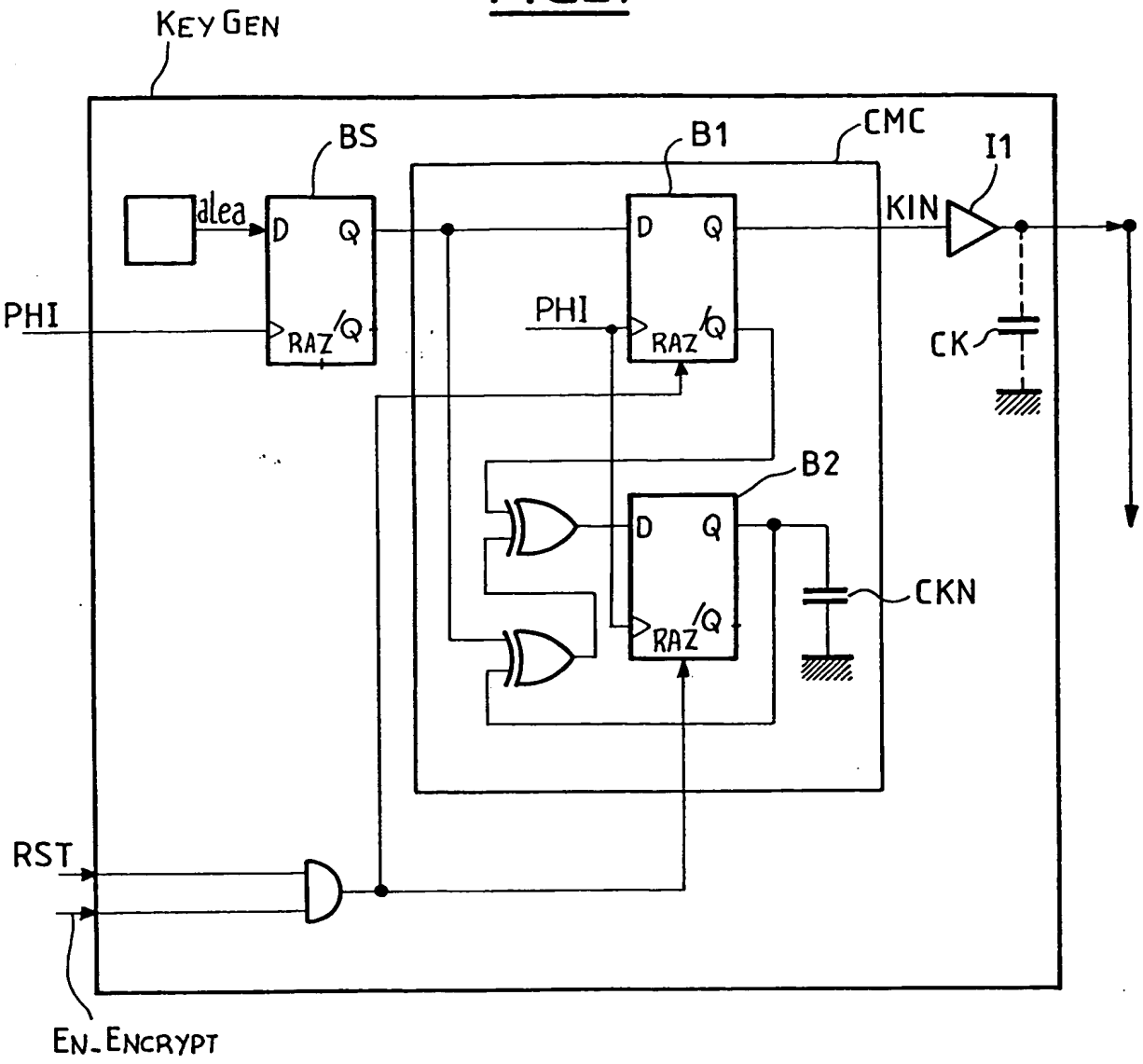

KEYREG
K0
E0
E1
E2
E3
E4
E5
E6
E7
KIN
PHI
(Dout0-Dout7)
K7
K6
K5
K4
K3
K2
K1
K0
A
Dout7
Dout6
Dout5
Dout4
Dout3
Dout2
Dout1
Dout0
PHI
DATA-BUS
Din7
Din6
Din5
Din4
Din3
Din2
Din1
Din0
B
Din0-Din7
K7
K6
K5
K4
K3
K2
K1
K0

FIG_7


KEY GEN
BS
B1
CMC
I1
dlea
D
Q
KIN
PHI
RAZ
/Q
CK
B2
CKN
RST
EN_ENCRYPT

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.